Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 09 April 2003

Current Nationwide Threat Level is

HIGH
High Risk of Terrorist Attacks

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports federal officials warn of chemical threats from commonly found chemicals that have legitimate uses in American industry. (See item 5)
- Federal Computer Week reports that according to projections based on a new U.S. Conference of Mayors survey, with the terror alert high and war raging in Iraq, U.S. cities are spending about $70 million weekly on additional homeland security measures. (See item 21)
- The Associated Press reports the hacker who invaded the computer system at William Bee Ririe Hospital in Ely, Nevada, has been traced to the former Soviet Union. (See item 23)
- CNET News.com reports the Samba Team released a patch on Monday for the second major security flaw found in the past few weeks in the open−source group's widely used program for sharing Windows files between Unix and Linux systems. (See item 24)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: High
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 08, Platts Global Energy News* — **World oil market currently over−supplied. World oil markets are currently over−supplied as no physical shortage has resulted from the war in Iraq and exports from OPEC members Nigeria and Venezuela have increased in recent days,** OPEC secretary−general Alvaro Silva said Tuesday. "The market is now oversupplied,

there is no shortage," Silva told Platts. Looking ahead to OPEC's hastily−arranged Apr 24 meeting in Vienna, Silva said the organization had to have "one eye on the war, and the other eye on supply and demand." **"The war did not produce a shortage, the market is going down. The market is oversupplied now," he said. "Venezuela is OK, they have started gasoline exports,"** Silva said, while the situation in Nigeria is also improving. OPEC ministers are expected to consider how to respond to the recent fall in oil prices, which has seen the price of OPEC's basket of seven crudes fall to $24.91/bbl Monday from over $32/bbl in mid−March. **One OPEC source said Thursday that the "most pragmatic" option for ministers would be to cut output at the Apr 24 meeting.**
Source: http://www.platts.com/stories/oil1.html

2. *April 07, Reuters* — **New head of U.S. nuclear agency plans safety changes. The Nuclear Regulatory Commission (NRC) will soon issue orders to improve the training of guards at U.S. nuclear power plants and to revise rules for nuclear fuel enrichment to prevent sabotage or attacks,** the new head of the agency said on Monday. Nils Diaz, who was appointed to the job of NRC chairman one week ago, said one of his top priorities is to improve security requirements for operating nuclear power plants. The agency has been focusing on tighter nuclear plant security since the Sept. 11, 2001, attacks on United States. Diaz said in a statement that the agency would soon issue orders "to enhance training and address security force fatigue." He did not elaborate. **Diaz also said the commission would "revise the design basis threats for operating nuclear power plants and Category 1 fuel cycle facilities later this month." Fuel cycle facilities are used to mill, convert, enrich and fabricate uranium to prepare it as a fuel. Last August, the NRC issued a proposal to improve the oversight of 10 U.S. fuel cycle facilities.** The NRC oversees the the nation's 103 operating nuclear power plants, which provide about 20 percent of the nation's electricity.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3756354

3. *April 07, Platts Global Energy News* — **NRC maintains full “red” finding at Point Beach, adds new one.** A previous "red" finding at Point Beach (near Manitowoc, WI) was not an "old design" issue, the Nuclear Regulatory Commission (NRC) decided, while issuing a preliminary red finding on a separate but possibly related matter. Both issues deal with the plant's auxiliary feedwater system. **Red−−the highest level in NRC's four−tier system−−denotes high safety significance. Under NRC's Reactor Oversight Process, a red finding would generally lead to a broad assessment of the plant's management.** If NRC had found the problem to be an old design issue−−as Nuclear Management Co. (NMC) contended last year −− NRC's response to the finding would have been scaled back. **But the agency ruled that NMC had failed to implement full corrective actions and that the performance deficiency that caused the first problem, which related to loss of instrument air, may have led to the second one, which concerned potential clogging of recirculation lines with water−borne debris.**
Source: http://www.platts.com/stories/nuclear1.html

[Return to top]

Chemical Sector

4. *April 08, Washington Post* — **Bush administration seeks voluntary chemical plant security steps.** The Bush administration is proposing new legislation to improve security standards at

chemical plants that will **emphasize voluntary compliance by an industry that some experts say is one of the nation's most vulnerable to catastrophic terrorist attack.** Sen. James M. Inhofe (R−OK) is working with the White House and the Department of Homeland Security to craft a bill that would require chemical companies to abide by standards drawn up by their industry association, rather than be subject to mandatory government measures advocated by environmental activists and many Democrats, officials said. **The Environmental Protection Agency has identified 123 chemical plants where a terrorist attack could, in a "worst−case" scenario, kill more than one million people.** Besides the airline industry, which tightened security as demanded by the U.S. government after the Sept. 11, 2001, attacks, the chemical industry is the first business sector that the administration has sought to regulate to lessen the danger of terrorism. Homeland Security officials are considering how to harden many elements of the nation's "critical infrastructure" −− which includes gas pipelines and water plants −− **and they say chemical plants are one of the most worrisome sectors.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A51903−2003Apr 7.html

5. *April 08, Associated Press* — **U.S. official warns of chemical threats. Nerve agents like VX and sarin gas are scary terrorist threats, but a top federal official is more worried about chemicals that travel the nation's highways every day.** "They are just as lethal," said Jerry Hauer, acting assistant secretary for public health preparedness at the Department of Health and Human Services. After the 1995 release of sarin gas in a Tokyo subway by the Aum Shinrikyo cult, government officials focused attention on nerve gases, **but now they are realizing the threat posed by chemicals that have legitimate uses in American industry,** Hauer said in an interview Monday with The Associated Press. "I just believe that at the end of the day, it's a lot easier getting something that's available here in the United States than trying to sneak in sarin," Hauer said. **For instance, toxic industrial chemicals such as chlorine, phosgene and hydrogen cyanide are readily available. These are among the earliest chemical weapons and were used by troops in World War I. Today, they are commonly used in commercial manufacturing, and experts believe they could easily be used for terrorism.** Cyanide, for instance, is used in electroplating, where metals are attached to each other, and jewelry manufacturing. It's readily available and has been used to attack the public before: In 1982, cyanide−laced capsules of Tylenol Extra Strength killed five people and terrorized the nation. **Hauer said law enforcement agencies are working with the chemical industry to improve security of transportation of chemicals and the safety of chemical facilities.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A53570−2003Apr 8.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *April 06, New York Daily News* — **Upstate charity tied to illegal Iraqi cash.** Federal agents have begun to unlock the secrets of an unlicensed, unregistered Islamic charity in upstate New

York that allegedly pumped millions of dollars into Baghdad. **Flouting U.S. economic sanctions, the group shipped cash out of Syracuse, laundered it in banks in Jordan and then illegally funneled it into Iraq, according to an unsealed federal indictment. Operating under the name Help the Needy, the organization described itself as a tax−exempt nonprofit that provided food and humanitarian assistance to the "starving children and suffering Muslims of Iraq."** But it lacked charitable status, misrepresented itself in appeals to donors, never got a license to send aid to Iraq, as required by federal law − and, more ominously, had ties to groups accused of supporting al Qaeda, investigators say.
Source: http://www.nydailynews.com/news/wn_report/story/73083p−67654 c.html

7. *April 06, Star−Ledger* — **Tracking Saddam's secret wealth.** It has been dubbed **"Saddam Inc.," a mysterious, multibillion−dollar empire that is said to have allowed Saddam Hussein and his sons to methodically stash away stolen riches in secret bank accounts around the globe.** Now, as the American military moves closer to toppling Saddam's regime in Baghdad, U.S. Treasury officials and intelligence agencies say they are scoring new successes in their effort to unravel and seize Saddam's hidden wealth. **"We have identified and located previously unknown assets that so far have exceeded $1 billion,"** David Aufhauser, general counsel for the Treasury Department, said in an interview. "We are now talking to these countries and are seeking to have them take measures to secure these funds for the repatriation of this wealth to the Iraqi people." **Bush administration officials say there is evidence that Saddam's fortune has come from smuggling, kickbacks and a variety of business deals engineered by his sons Uday and Qusay and other relatives.** The administration's financial task force is focusing on evidence that Saddam and his sons extorted huge kickbacks from foreign businessmen who participated in the Oil for Food program sanctioned by the United Nations.
Source: http://www.nj.com/news/ledger/index.ssf?/base/news−7/1049615 40911130.xml

[Return to top]

Transportation Sector

8. *April 08, The Advocate (Stamford, CT)* — **Metro−North train safety rolls along.** Transit officials say an advertising campaign encouraging commuters on Metro−North Railroad and elsewhere to report suspicious packages or people has increased awareness about potential terrorism threats. **Since launching its "If You See Something, Say Something" campaign last month, the Metropolitan Transportation Authority has reported a hike in the number of calls about suspicious behavior.** The ads coincided with the U.S.−led invasion of Iraq and the raising of the nation's terror alert level to orange, the second highest in the color−coded five−point scale. Although he had no numbers showing an increase in reports, MTA spokesman Tom Kelly said the campaign is working. **"We know it's a success simply because the interactions between customers and MTA Police, National Guardsmen or state troopers happens much more frequently than it ever did before,"** Kelly said. "This has given people a reason to be more communicative because this is something that we as a railroad and overall transit system are encouraging them to do."
Source: http://www.stamfordadvocate.com/news/local/scn−sa−mta2aapr08 ,0,7875802.story?coll=stam−news−local−headlines

9. *April 07, Federal Computer Week* — **TSA ramping up smart card tech.** The Transportation Security Administration (TSA) plans to begin testing technologies this month for an ambitious program that will equip 15 million transportation employees with smart cards, officials said. **TSA will soon launch two regional pilot projects for its Transportation Worker Identification Credential system. TWIC will provide employees at airports, seaports, railways and other locations with secure access to buildings and systems. Through a single network of databases, it will enable quick dissemination of threat alerts and revocation of access.** "This is really the start for being able to have a nationwide secure transportation system," said Randy Vanderhoof, executive director of the nonprofit Smart Card Alliance Inc. Interest in smart cards — plastic IDs with embedded computer chips that were first developed in the 1970s — soared after the Sept. 11, 2001, terrorist attacks, but progress slowed as Congress wrangled over the fiscal 2003 budget and as government officials awaited appropriations. **The technologies under consideration include cards that have a magnetic stripe, a two−dimensional bar code, a linear bar code, an optical memory chip or an integrated circuit chip,** she said. Additionally, TSA will explore incorporating a digital photo in conjunction with each of those options.
Source: http://www.fcw.com/fcw/articles/2003/0407/tec−tsa−04−07−03.a sp

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *April 08, Nature* — **Wool−free sheep to shave mutton costs. U.S. farmers are breeding wool−free sheep to bring down the cost of meat production.** Called hair sheep, the almost−bald animals don't need shearing, in contrast with parasite−prone woolly sheep. Kreg Leymaster, a geneticist with the U.S. Agricultural Research Service and his colleagues are crossing two breeds: the parasite−resistant Katahdin and the muscled Dorper. They hope that U.S. farmers will choose their low−maintenance hybrid over the woolly breeds from Australia and New Zealand. **"The primary advantage is decreased cost and labor for the ewe flock," says Leymaster.**
Source: http://www.nature.com/nsu/030407/030407−2.html

11. *April 08, Reuters* — **Chicken virus may have surfaced in Texas.** A highly contagious poultry disease that has forced health officials to kill more than 3 million chickens in the U.S. Southwest may have surfaced in Texas, state government officials said Tuesday. **The Texas Animal Health Commission said a flock of noncommercial chickens in El Paso was suspected of having Exotic Newcastle Disease.** If confirmed, Texas would be the fourth state infected since the outbreak started in October in southern California. Arizona and Nevada were also affected.
Source: http://www.forbes.com/business/newswire/2003/04/08/rtr932934 .html

[Return to top]

Food Sector

12. *April 08, Associated Press* — **USDA official: more being done on E. Coli.** The U.S. Department of Agriculture (USDA) has enacted several policies to better detect and track the deadly strain of E. coli bacteria in meat, a federal food safety official said. **Merle Pierson, USDA deputy undersecretary for food safety, told about 250 people at a meat safety conference Monday that federal inspectors have started regularly taking meat samples from all meatpacking plants.** In the past, federal inspectors usually took raw ground beef samples only from plants that did not do their own E. coli testing. **Last year, the USDA also implemented policies that require the gathering of records on a plant's suppliers if meat from the plant is presumed contaminated.** If meat from a plant tests positive for the deadly strain of E. coli, the plant's suppliers also must be notified, Pierson said.
Source: http://www.guardian.co.uk/uslatest/story/0,1282,−2542434,00. html

[Return to top]

Water Sector

13. *April 08, Orlando Sentinel* — **Cost of water security runs deep. All it took for someone to gain access to the water−treatment facility operated by Volusia, FL was to remove three bolts and push aside a section of chain−link fence.** After slipping through, the intruders tossed around equipment within the compound that provides water for roughly 15,000 people and damaged a conduit for security−system wires. County officials maintain that the January break−in was random vandalism, but it pointed out security vulnerabilities that some experts say exist at many water plants across the country. **With the nation on guard like never before for acts of terror, industry officials say public and private utilities have a long way to go to provide the level of security expected at water plants.** The amount spent to protect drinking water pales in comparison with money that has gone toward beefing up security at other possible terror targets.
Source: http://www.orlandosentinel.com/news/local/volusia/orl−locwat ersecurity08040803apr08,0,3570196.story?coll=orl−news−headli nes

[Return to top]

Public Health Sector

14. *April 08, BBC News* — **SARS spread by cockroaches. Experts have a new theory on how the Sars illness raced through an entire apartment block in Hong Kong. They believe that cockroaches may have carried the infection from flat to flat.** The cockroach theory was voiced by Hong Kong Deputy Director of Health Leung Pak−yin on Monday. He was talking about how the disease managed to spread like wildfire through an apartment block at Amoy Gardens in Kowloon. **In just a few days, more than 300 new cases arose among residents of the block.** The cases left health officials baffled and deeply concerned, as many of the 300 had had no direct contact with anyone who had Sars. Leung said: "The drainage may be the reason.

"It is possible that the cockroaches carried the virus into the homes."
Source: http://news.bbc.co.uk/2/hi/health/2927695.stm

15. *April 08, Time* — **Doctor and party member insists there are more SARS cases than officials admit. A physician at Beijing's Chinese People's Liberation Army General Hospital in a signed statement, says that at one Beijing hospital alone, 60 Severe Acute Respiratory Syndrome (SARS) patients have been admitted of whom seven have died.** That indicates the number of patients infected with SARS in Beijing may be significantly higher than those totals made public by China's Ministry of Health. Last Thursday Chinese Minister of Health Zhang Wenkang announced to the press that China's capital had seen just 12 cases of SARS of whom three had died. **Tuesday's edition of the official China Daily put the number of SARS infections in Beijing at 19 with four dead.**
Source: http://www.time.com/time/asia/news/daily/0,9754,441615,00.ht ml

16. *April 07, University of Wisconsin* — **Researchers find second anthrax toxin receptor.** Building on their 2001 discovery of a cellular doorway used by anthrax toxin to enter cells, University of Wisconsin Medical School researchers have found a second anthrax toxin doorway, or receptor. The finding could offer new clues to preventing the toxin's entrance into cells. **The researchers also have found that when they isolated a specific segment of the receptor in the laboratory, they could use it as a decoy to lure anthrax toxin away from the real cell receptors, preventing much of the toxin from entering cells and inflicting its usually fatal damage.**
Source: http://www.news.wisc.edu/releases/view.html?id=8478ront>

17. *April 06, Independent* — **Disease may change to an even deadlier form. Reinhard Kurth, the head of the German government's Robert Koch Institute, was not exactly encouraging on Friday night. A vaccine for Severe Acute Respiratory Syndrome (SARS) could be developed, he said, but it would take three to five years.** Experts worldwide are still struggling to identify what is causing the illness, and how it is transmitted. Some can already see light at the end of the tunnel. "To me, the epidemic is almost certainly over," said Osman David Mansoor, a World Health Organization (WHO) scientist. "But there is always a lag time for infections. While we are speaking there may be a whole other lot of infections going on." **The possibility is that SARS will die out after failing to transmit itself, before any cure beyond acute medical care can be devised. But the lurking fear is still that it might find a way to revive itself, like the Spanish flu epidemic which spread throughout the world from a military camp in Kansas in 1918.** The similarities with the 1918 flu pandemic are quite striking. True, the mortality rate among those infected with Sars peaked at around 4 per cent, and doctors are getting better at treating it. The 1918 influenza strain at times killed 28 percent of those infected, but its overall mortality rate was 2.5 percent.
Source: http://news.independent.co.uk/world/science_medical/story.js p?story=394456

[Return to top]

Government Sector

18. *April 08, Government Computer News* — **Open−source directory seeks info about**

government projects. The Center of Open Source and Government this fall will publish a directory of open−source projects within agencies and large companies. The Open Source Resource Book 2003 will provide a "who's doing what" list of development efforts, said Tony Stanco, director of the center, which is an affiliate of the Cyber Security Policy and Research Institute at George Washington University. Listings are free, Stanco said. Representatives of government agencies and national laboratories can go to the reference book's home page, at www.egovos.org/ref_book.html, to complete an online questionnaire for a listing. **The directory will include a list of mature open−source software generally regarded as safe, plus a year−in−review section and a listing of open−source conferences. The deadline for submitting listings is May 31**. Stanco said he would release the reference book in November at the third Open Source in Government conference in Paris. The center plans to update the directory annually, Stanco said.
Source: http://www.gcn.com/vol1_no1/daily−updates/21646−1.html

19. *April 07, Government Executive* — **HSD readies antiterror watch list.** The Homeland Security Department (HSD) soon will unveil a governmentwide watch list of suspected terrorists, achieving what secretary Tom Ridge designates as the new department's No. One IT goal. **"We have several departments and units that developed their own watch lists," the Homeland Security secretary said last week. "Our first IT priority is to consolidate those watch lists so people at the borders and airports and respective agencies can access that broader list of names−the aggregate of these names."** The effort is well under way, Ridge said. "We are moving rapidly to a point where we can tell you it's done. We are not quite there yet, but we will be there shortly," he said. Ridge spoke at a press briefing where he and British Home secretary David Blunkett unveiled efforts for the two organizations to coordinate counterterrorism programs. **The government's terrorist watch lists sometimes are referred to as watchout lists to avoid confusion with the term the Navy uses for duty rosters.**
Source: http://www.gcn.com/22_7/homeland−security/21613−1.html

20. *April 07, Government Executive* — **Few agencies outside Washington buy antiterror gear for employees.** As federal agencies craft plans to protect their employees from terrorism, few offices outside Washington are buying protective hoods that could help employees escape a chemical, biological, or radiological attack, according to federal officials. In Washington, the Agency for International Development is providing its headquarters employees with escape hoods, joining the Defense Department and Office of Personnel Management as agencies that have outfitted their Washington−area employees with protective hoods or breathing masks. The Capitol Police distributed 25,000 hoods to congressional staff and members of Congress last fall. **But outside the nation's capital, the question of whether to buy hoods has stirred less debate. In many regions, it is not a major concern of federal preparedness planners. "We've not planned for the hoods here in Oklahoma," said LeAnn Jenkins, director of the Federal Executive Board in Oklahoma City, Okla., which has published several guides to help federal agencies prepare for possible terrorist attacks. In New York City, officials were unaware of any federal agencies that were buying hoods.** "We would know if somebody were proposing to do that, but I have not heard of any effort," said Michael Beeman, a spokesman with the Federal Emergency Management Agency in New York. Cynthia Gable, executive director of the Federal Executive Board in New York, said she had not heard of any federal agencies in New York purchasing hoods.
Source: http://www.govexec.com/dailyfed/0403/040703p1.htm

21. *April 07, Federal Computer Week* — **High alert status costs cities.** With the terror alert high and war raging in Iraq, U.S. cities are spending about $70 million weekly on additional homeland security measures, according to projections based on a new U.S. Conference of Mayors survey. **Baltimore Mayor Martin O'Malley called on the federal government to share the costs of homeland security and provide direct funds to municipalities rather than funnel them through state governments.** The expenditures are direct costs, mostly for overtime pay, O'Malley said, and don't account for extensive equipment and training needs. O'Malley said cities aren't asking the federal government to "pay for year−round maintenance, training, recruitment, deployment" of first responders, but he added that America's cities shouldn't shoulder the burden themselves. **The national conference, which represents cities with populations of 30,000 or more, surveyed 145 politically and geographically diverse cities ranging in population from 21,000 to 8 million.**
Source: http://www.fcw.com/fcw/articles/2003/0407/pol−cities−04−07−0 3.asp

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

22. *April 08, Next* — **Australia leaves the hack door open to cyber sabotage. Australia's critical information infrastructure is at risk because of the Federal Government's focus on physical infrastructure and terrorism, the head of Australia's Computer Emergency Response Team (AusCERT) says**. AusCERT general manager Graham Ingram says that **Malaysia, South Korea and Japan are spending enormous amounts of money on protecting information infrastructure − things such as government, banking, public utility, telecommunications and emergency networks. In Australia, many of these assets are in private hands**. AusCERT has been contracted by the Federal Government to provide a free service to the general public and business about new threats to networked computer systems as part of the Trusted Information Sharing Network (TISN). TISN is a voluntary forum for owners of critical infrastructure to exchange information on security issues announced last November. But Kate Lundy, IT spokeswoman for Australia's Labor Party, says **laws are needed to force the private sector to comply with minimum standards of protection for critical information infrastructure**.
Source: http://www.smh.com.au/articles/2003/04/07/1049567603965.html

23. *April 07, Associated Press* — **Ely hospital hacker traced to former Soviet Union. A hacker who invaded the computer system at William Bee Ririe Hospital in Ely, Nevada, has been traced to the former Soviet Union**, authorities said. **The FBI said the hacker used the Web site of Al−Jazeera, the Arab news network, as a conduit to the hospital**. Officials at the hospital said patient records are safe, but added that the cyber intruder may have accessed employee Social Security and bank information. Jim Crosley, information technology manager

for the Ely hospital, detected the Ely break−in on March 20. He said the system seemed to be protected from attacks, but **the FBI lab's analysis of the hospital's hard drives showed a game program, "Blaster Ball," contained a Trojan horse, a hidden code that acted as a beacon and let hackers into the hospital's system. "Two employees admitted downloading the game from the Internet and installing it at a work station**," Crosley said. "The Trojan horse reported back to the hackers, and the system was compromised."
Source: http://www.lasvegassun.com/sunbin/stories/nevada/2003/apr/07 /040710833.html

24. *April 07, CNET News.com* — **Samba flaw threatens Linux file servers. The Samba Team released a patch on Monday for the second major security flaw found in the past few weeks** in the open−source group's widely used program for sharing Windows files between Unix and Linux systems. **The security problem could easily let an attacker compromise any Samba server connected to the Internet. The vulnerability is already being used by online attackers to compromise vulnerable servers**, the company warned in an advisory. **The Samba software that runs on major Linux distributions as well as FreeBSD and Sun Microsystems' Solaris operating system were affected**. Security firm Digital Defense found the vulnerability. However, in an added twist to the situation that could make the threat more serious, while Digital Defense noted that some hackers obviously knew of the method by which the vulnerability could be exploited, it also mistakenly posted its own exploit onto its Web site. **A patch is available on the Samba Website: http://us1.samba.org/samba/samba.html.**
Source: http://news.com.com/2100−1002−995834.html

25. *April 07, Computerworld* — **Handle corporate security as single entity, users say. Companies can improve their ability to detect and respond to both cyber and physical threats by tying their IT security to other aspects of corporate security**. But the cultural and business−process changes involved in implementing such a holistic view of security can be daunting for most corporations, users said here last week at a conference organized by ASIS International, an organization of security professionals. Lew Wagner of the MD Anderson Cancer Center at the University of Texas in Houston, said coordinating IT security functions with areas such as physical protection, facilities management, human resources and legal and audit functions has helped enhance overall threat−detection and incident−response capabilities at the hospital. **A holistic view of enterprise security can help plug gaps that might otherwise be missed**, said James Litchko, of Litchko & Associates Inc., a security consultancy in Kensington, MD. For instance, **the majority of IT−related security threats still stem from procedural and process flaws−such as failure to secure access to crucial systems, inadequate backups and lack of auditing−rather than from technology glitches**, Litchko said.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,80069,00.html

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 25 (smtp), 113 (ident), 445 (microsoft−ds), 139 (netbios−ssn), 53 (domain), 4662 (eDonkey2000), 1214 (kazaa) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

26. *April 08, Associated Press* — **New purported bin Laden tape urges suicide attacks.** A new cassette tape purported to be from Osama bin Laden urges suicide attacks and calls on Muslims to rise up against Arab governments that support the attack on Iraq. **In the audio tape, bin Laden's supposed voice urges the faithful to attack the governments of Pakistan, Afghanistan, Bahrain, Kuwait and Saudi Arabia. Unlike previous such tapes, this one had a single theme − suicide attacks. "All of them have been imposed upon you and jihad (holy war) against them is your duty," the Arabic language tape received Monday in remote northwestern Pakistan said.** The tape was obtained by The Associated Press from an Algerian national, identified only as Aadil, who said he had slipped across the border from Afghanistan, where the bin Laden tape was apparently recorded. **There was no way to independently confirm that the voice on the tape was that of bin Laden, but it was translated by an Arabic speaking Afghan who met with the terrorist mastermind years ago and who said the voice appeared to be his.**
Source: http://www.usatoday.com/news/world/2003−04−08−osama_x.htm

27. *April 08, USA Today* — **Many types of businesses feel war's impact.** The war is rippling through the economy, affecting companies far from the fighting. **About 8% of the nearly 8,000 companies that filed annual reports with the Securities and Exchange Commission this year say the war has affected or could affect them, says research firm 10K Wizard.** The bulk of the reports were filed in recent weeks. Many warnings were expected. Airline and oil companies saw an immediate impact on business. But companies in seemingly unrelated industries say they're vulnerable, also.
Source: http://www.usatoday.com/money/world/iraq/2003−04−06−warnings_x.htm

28. *April 08, Los Angeles Times* — **Jemaah Islamiah terrorists tied to two blasts.** The Jemaah Islamiah terrorist group, which allegedly carried out the deadly Bali bombing on October 12, is

suspected of involvement in two recent blasts in the southern Philippines that killed 37 people, Philippine authorities said Monday. **National police intelligence chief Roberto Delfin said five alleged members of the militant Muslim group are being sought in an April 2 blast in Davao City that killed 16 people near a crowded wharf.** Delfin said the Southeast Asian terrorist network also is suspected in a March 4 bombing that killed 21 people outside the Davao City airport passenger terminal. Jemaah Islamiah is accused of carrying out dozens of bombings in Southeast Asia since 2000 in a campaign to establish a separatist Islamic state in the region. The Bali nightclub bombings, which killed 202 people was Jemaah Islamiah's biggest attack. **Authorities say the group is affiliated with Osama bin Laden's al Qaeda terrorist network, which allegedly has helped finance and direct some of the regional group's terrorist activities.**
Source: http://www.latimes.com/news/nationworld/world/la−fg−phil8apr08002429,1,3716068.story?coll=la%2Dheadlines%2Dworld

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer